



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,414	03/03/2004	Jing Xiang	NRT.0124US	2562
21906 7590 01/22/2008 TROP PRUNER & HU, PC 1616 S. VOSS ROAD, SUITE 750 HOUSTON, TX 77057-2631			EXAMINER TABOR, AMARE F	
			ART UNIT 2139	PAPER NUMBER
			MAIL DATE 01/22/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/791,414

Applicant(s)

XIANG ET AL.

Examiner

Amare Tabor

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 09 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9-12, 14, 17 and 20-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7, 9-12, 14, 17 and 20-22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This correspondence is in response to amendment filed on November 09, 2007.
2. Claims 1, 7, 9-11, 14 and 17 are amended; Claims 8, 13, 15, 16, 18 and 19 are cancelled; Claims 2-6 and 12 are original; and Claims 20-22 are new.
3. Claims 1-7, 9-12, 14, 17 and 20-22 are pending

### *Response to Arguments*

4. Applicant's arguments filed on 11/09/2007 have been fully considered but they are not persuasive.

Regarding Claim 1, Applicant argued that "*Ahonen clearly does not contemplate that both old and new addresses are communicated in the control authorization certificate.*"

Examiner respectfully disagrees. Ahonen discloses that the authorization certificate include SAs consisting: (i) the "original" Source and Destination IP addresses if the mobile host is "physically" located in intranet 5 (*par. [0097] to [0105]*); and, (ii) the (New) Source and Destination IP addresses (if changed) if the mobile host is remotely accessing to intranet 5 (*par. [0106] to [0118]*). Furthermore, the firewall 3 compares every incoming packet with the content the RCDB (*par. [0133] to [0143]*). Thus, old and new information about the packet is communicated in the process of firewall investigating packets by comparing distinct fields (including the Source and Destination IP addresses).

Regarding Claim 10, Applicant argued that "*establishing multiple security associations among the mobile host, firewall, and multiple correspondent hosts does not constitute duplicating (at a third network element) information associated with a secure network connection between a first network element a second network element.*"

Examiner respectfully disagrees. In the preparation function of Phase 1 and 2 (*paragraphs [0047]-[0048] and [0087] to [0088]*), Ahonen discloses that the ISKAMP SA is negotiated between mobile host 1 and firewall 3 first, and the negotiation process is repeated between mobile host 1 and correspondent host 4. In other words, the first ISKAMP SA between the first and second network elements (mobile host and firewall) is duplicated by repeating the security association negotiation process between the first network and the third elements (mobile and correspondent host).

Regarding Claim 12, Applicant argued that "*nowhere in this passage of Ahonen [Office Action cited paragraphs 0012 and 0035] is there any hint of sharing at least one security association among the plurality of security gateways.*"

Examiner respectfully disagrees. Ahonen discloses that the Virtual Private Network (VPN) may involve one or more corporate LANs (see *Fig. 1 and paragraph [0002] and [0035]*). Therefore, it is obvious to a person of ordinary skill in the art to expand the system of Ahonen to share SAs among plurality of security gateways.

Regarding the newly added Claim 22, please see rejection of the Claim below.

5. Applicant's arguments with respect to the pending claims are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**Claims 1-7, 9, 10, 20 and 21 rejected under 35 U.S.C. 102(b) as being anticipated by "Ahonen," (US Pub. No.: 2001/0009025 A1, now US Pat. No.: 6,976,177 B2).**

***As per Claim 1***, Ahonen teaches,

A method for maintaining secure network connections (see *Fig. 1-5 and abstract*; and for example, *par. [0004] to [0011]*), the method comprising: detecting a change of address from an old address to a new address associated with a first network element (see *the mobile host 1 in Fig. 1*; and for example *par. [0010], [0012], [0098], [0109], [0111] to [0113], [0124], [0129], [0133] and [0134]*);

updating at least one first security configuration at the first network element (see *Fig. 2-4 and abstract*; where *the authentication certificate is updated at the mobile host*; and for example, *par. [0006] to [0011] and [0019] to [0023]*);

transmitting at least one secure message from the first network element to a second network element (see *Fig. 2-4*; where *secure messages, such as: ISKAMP SA, IPSec SA #1/#2, Proposal, etc. are transmitted between Peer 1/Initiator and Peer 2/Responder*),

wherein the at least one secure message contains both the old address and the new address (see for example, par. [0097] to [0105] and [0111] to [0118]; where the control authorization certificate sent from the mobile host to the firewall consists the (New) Source and Destination addresses (if changed)), wherein the old address and the new address in the at least one secure message enables at least one second security configuration at the second network element to be updated (see Fig.5; and where certificate is sent from mobile host to firewall, and firewall authorizes mobile host; and for example, Remote Control Function form par. [0108] to [0129]).

***As per Claim 9,*** Ahonen teaches,

At least one processor readable-medium for storing a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 1 (see Fig.2-5 and abstract; and for example, par.[0019] to [0023] and [0035]; where means for storing computer program instructions"daemons" and inherent processor in the mobile host 1 or security gateway/firewall 3 and server/correspondent host 4 are disclosed).

***As per Claim 10,*** Ahonen teaches,

A method for maintaining secure network connections (see Fig.1-5 and abstract; and for example, par.[0004] to [0011]), the method comprising: duplicating, at a third network element (see server/correspondent node 4 in Fig.4), information associated with a secure network connection between a first network element and a second network element (see Fig.2-3; where in Phase 1 and 2, par.[0047] and [0088], the ISKAMP SA is negotiated between mobile host 1 and firewall 3 first, and the negotiation process is repeated between mobile host 1 and correspondent host 4; and for example, abstract, par. [0001], [0005] to [0011], [0037], [0096] to [0099] and [0108] to [0129]), wherein a lookup of security associations associated with the secure network connection is not dependent on any destination address (the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address; see for example, par. [0012], [0106], [0119] to [0122]); and

in response to detecting failure of the second network element, replacing the second network element with the third network element in the secure network connection with the first network element (communication between mobile and correspondent host through the security gateway/firewall 3 is disclosed as "preferable"; see for example, par. [0004] to [0015]; a separate negotiation process between mobile host and correspondent node is established; see for example, Fig.2-3; and par. [0047] and [0088]; furthermore, during mobile host's remote access to intranet 5 in Fig.1, the server/correspond host may replace the firewall/security gateway 3; see for example, par. [0108], [0146] to [0156]).

***As per Claim 2***, Ahonen teaches,

wherein a lookup of security associations is not dependent on any destination address (*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address; see for example, par. [0012], [0106], [0119] to [0122]*).

***As per Claim 3 and 21***, Ahonen teaches,

wherein the first network element is a mobile client and the second network element is a security gateway (see *mobile host 1 and security gateway 3 in Fig. 1*); and

the second and third network elements are security servers (see *security gateway 3 and correspondent node/server in Fig. 1*; and for example, *par. [0035]*).

***As per Claim 4***, Ahonen teaches,

wherein the first network element and the second network element are part of a virtual private network (VPN) (see *abstract and Fig. 1*; and for example, *par. [0001], [0005], [00013] and [0029]*).

***As per Claim 5***, Ahonen teaches,

wherein communications between the first network element and the second network element are based on a security architecture for the internet protocol (IPsec); and wherein communications between the mobile client and the first security server are based on a security architecture for the internet protocol (IPsec) (see *SAs based on IPsec in Fig. 2 and 4*).

***As per Claim 6***, Ahonen teaches,

wherein at least part of the communications between the first network element and the second network element are based on an internet security association and key management protocol (ISAKMP) (see *SA based on ISAKMP in Fig. 2*).

***As per Claim 7***, Ahonen teaches,

the second network element identifying at least one security association based on at least one cookie field in the at least one secure message (see for example, *par. [0055], [00119] to [0127] and [0133] to [0137]; where the second network element; i.e., the firewall, identifies the SA based on the cookie field*).

*As per Claim 20*, Ahonen teaches,

during life of the secure network connection between the first and second network elements, the third network element receiving information relating to one or more security associations of the secure network connection from the second network element (see *Fig. 1 and abstract*; and for example, *par. [0001], [0007] and [0008]*; where the third network element; i.e., correspondent host receives information about the SAs from the second network element; i.e., the firewall).

### ***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 11, 12, 14, 17 and 22 rejected under 35 U.S.C. 103(a) as being unpatentable “Ahonen” in view of Shapira et al. (US Pub. No.: 2004/0117653 A1), referred as “Shapira” hereinafter.**

*As per Claim 12*, Ahonen teaches,

A method for maintaining secure network connections (see *Fig. 1-5 and abstract*; and for example, *par. [0004] to [0011]*), the method comprising: configuring a security gateway (see *firewall/Security Gateway 3 in Fig. 1*) such that a lookup of security associations is not dependent on any destination address (*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address*; see for example, *par. [0012], [0106], [0119] to [0122]*); and

sharing at least one security association with security gateway (see *abstract and Fig. 1-4*; where a security association is shared between the firewall, the mobile and correspondent hosts).

Ahonen does not explicitly disclose plurality of security gateways and sharing security association among the plurality of security gateways. However, in the same field of endeavor, Shapira discloses plurality of security gateways and sharing security association among the plurality of security gateways (see *Fig. 1*; and for example, *par. [0014] to [0019]*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to combine the teachings of Shapira and Ahonen because both inventions are directed to security association in VPN. One having ordinary skill in the art would be motivated to modify the system of Ahonen by adding one or more security gateways and share SAs of among plurality of security gateways as taught by Shapira because VPN of Ahonen may involve one or more corporate LANs (see *Fig. 1 and paragraph [0002] and [00035]*).

*As per Claim 22*, Ahonen teaches,

A first security server (see *Security Gateway/firewall 3 in Fig. 1*);

in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection; and communicate with the mobile client using the at least one security association over the secure network connection between the first security server and the mobile client (*communication between mobile and correspondent host through the security gateway/firewall 3 is disclosed as "preferable"; see for example, par. [0004] to [0015]; a separate negotiation process between mobile host and correspondent node is established; see for example, Fig. 2-3; and par. [0047] and [0088]; furthermore, during mobile host's remote access to intranet 5 in Fig. 1, the server/correspond host may replace the firewall/security gateway 3; see for example, par. [0108], [0146] to [0156]*).

Ahonen does not explicitly disclose a transceiver to receive information relating to at least one security association of a secure network connection between a mobile client and a second security server. However, Ahonen discloses a means for receiving information relating to at least one security association of a secure network connection between a mobile client and a second security server (see for example, *par. [0019] to [0024]*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants invention to conclude that the system of Ahonen has an inherent transceiver because means for receiving one more security association that is related to mobile host and firewall is disclosed (see *Fig. 2-4*)

Ahonen does not explicitly disclose a processor module to monitor operation of the second security server. However, Shapira discloses a processor module to monitor operation of the second security server (see *Security processor 88 in Fig. 3*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to incorporate the Security processor of Shapira into the VPN of Ahonen in order to monitor and enhance the security system by adding additional servers as a backup.



*As per Claim 11*, Ahonen teaches,

sending at least one secure message from the third network element to the first network element (see Fig.2-3; where in Phase 1 and 2, par.[0047] and [0088], the ISKAMP SA is negotiated between mobile host 1 and firewall 3 first, and the negotiation process is repeated between mobile host 1 and correspondent host 4; and for example, abstract, par. [0001], [0005] to [0011], [0037], [0096] to [0099] and [0108] to [0129]).

Ahonen does not explicitly disclose notifying the first network element that the secure network connection will be taken over by the third network element. However, Ahonen discloses exchanging at least one secure message between Peer 1 and Peer 2 (or Initiator and Responder) (see Fig.2-4). It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to conclude that the mobile host will be notified if the secure network connection will be taken by the correspondent node because Peer 1/Initiator and Peer2/Responder of Ahonen could act as first and third network element (see for example, par. [0004] to [0015], [0108], [0146] to [0156]).

*As per Claim 14*, Ahonen teaches,

wherein a lookup of security associations is not dependent on any destination address (*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address*; see for example, par. [0012], [0106], [0119] to [0122]).

*As per Claim 17*, Ahonen teaches,

wherein communications between the first network element (mobile client) and the second network element (first security server) are based on a security architecture for the internet protocol (IPsec) (see *SAs based on IPSec in Fig.2 and 4*).

### **Conclusion**

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor  
AU 2139

  
**AYAZ SHEIKH**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**